

5 FAM 870 NETWORKS

*(CT:IM-155; 09-22-2014)
(Office of Origin: IRM/BMP/GRP/GP)*

5 FAM 871 ENTERPRISE NETWORKS

(CT:IM-138; 01-18-2013)

The Department currently has two enterprise networks: ClassNet and OpenNet. Only Department-issued or approved systems are authorized to connect to Department enterprise networks.

5 FAM 871.1 ClassNet

(CT:IM-150; 05-01-2014)

- a. The Department's ClassNet provides an internal network for e-mail and other processing of information up to the SECRET level and provides access to the Department of Defense (DOD) Secret Internet Protocol Router Network (SIPRNET).
- b. Submit all ClassNet changes (i.e., baseline and modifications) to the Information Technology Configuration Control Board (IT CCB) for review, evaluation, and decision.
- c. Users must not load classified information or Sensitive But Unclassified (SBU) information onto unclassified systems, and any information exchange between classified and unclassified or SBU systems may only occur following established Department guidelines, developed by the Bureau of Diplomatic Security (DS), or with a recommended waiver by DS and approved by the Chief Information Security Officer (CISO).
- d. Users have no expectation of privacy when using Department systems. The system is monitored at all times for user actions and data classification.
- e. Only Department-owned and IT CCB-approved hardware (including removable media) and software are permitted to be installed or used on classified Department automated information systems (AISs). Computers connected to ClassNet must have all Department-required software patches applied and must have current anti-virus software and definitions installed. Additionally, portable computers must not connect to ClassNet systems without explicit approval of the bureau or post Information Systems Security Officer (ISSO). See 12 FAM 630 for additional security requirements.

5 FAM 871.2 OpenNet

(CT:IM-150; 05-01-2014)

- a. OpenNet is the Sensitive but Unclassified (SBU) network in the Department. It provides access to standard desktop applications, such as word processing, e-mail, and Internet browsing, and supports a battery of custom Department software solutions and database management systems.
- b. Submit all OpenNet changes (i.e., baseline and modifications) to the Local Configuration Control Board (LCCB) for initial review and evaluation. The change may be approved by the LCCB or sent via unclassified e-mail to their voting sponsor and IT CCB management for final review, evaluation, and decision, per IT CCB standard operating procedure (SOP) guidelines. See 5 FAM 862 for more information regarding LCCB processes and responsibilities.
- c. Users sending personal e-mail out to the Internet should make it clear, in an appropriate place in the message, that his or her e-mail is not being used for official business.
- d. Users must not load classified information onto unclassified or SBU systems, and any information exchange between classified and unclassified or SBU systems may only occur following established Department guidelines, developed by Diplomatic Security (DS) or with a recommended waiver by DS and approved by the Chief Information Security Officer (CISO).
- e. Users have no expectation of privacy when using Department systems. The system is monitored at all times for user actions and data classification.
- f. Only Department owned and IT CCB or LCCB approved hardware (including removable media) and software are permitted to be installed or used on SBU Department AISs. (All operating system software must be IT CCB approved.) Computers connected to the OpenNet must have all Department required software patches applied and must have current anti-virus software and definitions installed. Additionally, portable computers must not be connected to OpenNet systems without explicit approval of the bureau or post information system security officer (ISSO). See 12 FAM 620 for additional security requirements.
- g. For specific guidance on transport and use of portable computers at post, contact the Office of Computer Security (DS/SI/CS).

5 FAM 872 DEDICATED INTERNET NETWORKS (DIN)

(CT:IM-150; 05-01-2014)

A Dedicated Internet Network is dedicated Internet access from an Internet Service Provider (ISP) on a Department owned and operated discrete non-

UNCLASSIFIED (U)

sensitive unclassified local area network that is not connected to any other Department system. DINs are not protected by DOS Enterprise security services, e.g., boundary defense, data loss prevention, antivirus and vulnerability monitoring. ISP connections for the sole purpose of maintaining IRM/OPS/ENM/ND managed virtual private network (VPN) for contingency access to OpenNet are not considered DINs.

5 FAM 872.1 DIN Authorization and Registration

(CT:IM-150; 05-01-2014)

- a. Domestically, Bureau Executive Directors or equivalents are the approving authority for all DINs within their organization area of operation. Overseas, Management Officers are the approving authority for all DINs established within their post or mission. The Approving Authority must ensure DINs are only established for purposes which cannot be accomplished on OpenNet and that DINs are registered, supported and maintained in accordance with applicable Department policies and standards.
- b. To ensure all connections into Department of State facilities are documented, DINs must be registered with the Enterprise IT Configuration Control Board using the IT CCB DIN Registration site.
- c. DIN Approving Authorities or their designates must update DIN registrations annually on the IT CCB DIN Registration site in order to retain DIN authorization and insure accuracy of information.
- d. ISP connections that do not require registration with the IT CCB are:
 - (1) Commercially funded ISP connections, for instance ISP connections approved for tenant concessionaires.
 - (2) ISP connections and their networks that are funded by Public Affairs or other grants, that are not located on US Government property. An example would be an American Corner at a University.
 - (3) Personal residential ISP connections.
- e. Information required for the DIN registration is found on the IT CCB DIN site, includes:
 - Title/Registration Name
 - Fully Described Purpose of the DIN
 - Post\Bureau Name
 - Approving Authority Name and Title
 - ISSO
 - Technical Point of Contact (POC)
 - Description of Location

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 5
Information Management

- DIN type (wired, WI-FI or hybrid)
- Hardware and Software Configurations
- Number and Type of Equipment Used
- iTAB registration IDnumber from iMatrix

5 FAM 872.2 Acceptable Use

(CT:IM-150; 05-01-2014)

- a. Department Sensitive but Unclassified (SBU) information and Department Personally Identifiable Information (PII) must not be processed, stored or transmitted on DINs, except in limited amounts under exigent circumstances (i.e., OpenNet or other Department-provided secure means are not available). Under such circumstances, Department SBU information and PII may be transmitted on a DIN but must be immediately removed from the DIN after transmission. See 12 FAM 544.3, Electronic Transmission via the Internet.
- b. DINs must not be used to duplicate DOS Enterprise services that are available on OpenNet.
- c. Typical uses of DINs include:
 - Internet access for tenant agencies or organizations
 - Public Internet access
 - Software development and testing
 - Consular Affairs kiosks
 - Distance Learning
 - Downloading large files, device drivers, purchased software
 - Connections by GSO to banks that use special encryption
 - Use of software that cannot securely be used on OpenNet
 - Intermittent applications that require such high bandwidth that OpenNet would be degraded for other business use.

5 FAM 872.3 DIN Hardware and Software

(CT:IM-150; 05-01-2014)

- a. Only Department- owned and approved software must be used on DINs. The software must be legally procured and fully licensed, according to Department acquisition policies and vendor End User License Agreements. This software restriction does not apply to Internet Resource Center (IRC) or Department Hotspot client user devices.
- b. All Department purchased IT hardware and software must comply with all

UNCLASSIFIED (U)

federal accessibility laws and policies.

- c. All DIN hardware and software must be approved by either the Post, mission, or organization Local Configuration Control Board according to 5 FAM 115.6-2 Local Configuration Control Board (LCCB) or the enterprise Information Technology Configuration Control board (IT CCB), as appropriate. This hardware restriction does not apply to Internet Resource Centers (IRC) or Department Hotspot client user devices.
- d. DIN hardware and software must be configured to Department security configuration baseline standards, when possible. When baseline configurations must be adjusted to accommodate business requirements, they must be documented and maintained through the LCCB.

5 FAM 873 DEMILITARIZED ZONE (DMZ)

(CT:IM-155; 09-22-2014)

- a. *A DMZ is a perimeter network segment that is logically between internal and external networks. Its purpose is to enforce the internal network's information assurance policy for external information exchange and to provide external, trusted and untrusted sources with restricted access as required to releasable information while shielding the internal networks from outside attacks.*
- b. *The processing of Department data and information is subject to adherence to applicable Department and federal compliance standards.*
- c. *DMZs must not be established and/or operated without Chief Information Officer (CIO) authorization. The IRM Perimeter Security Division (IRM/OPS/ENM/PSD) maintains governance and oversight with the Department of State DMZs. Data in a DMZ may be accessed by untrusted sources that are not authenticated. Technical administration must be performed by a cleared U.S. citizen, Department of State or contract employees.*
- d. *Connectivity to, through, and from the DMZ, which includes systems, devices, networks, and proxies, is subject to general 5 FAM Automated Information System (AIS) and 12 FAM 600 cyber security policies and, therefore, must meet and maintain Department and Federal Information Security Compliance, related Department and Federal Information Technology, and data protection requirements and standards.*
- e. *Applications categorized as "high" are not authorized in the DMZ.*
- f. *DMZs must meet the following additional requirements:*
 - (1) *Only IRM may implement and operate a DMZ network segment between enterprise networks and external networks. All DMZs regardless of ownership will comply with the requirements of this section;*
 - (2) *Any data at rest in a DMZ system or application that has been categorized moderate must be encrypted using Department approved U.S. government*

certified encryption products;

- (3) DMZ's operating between enterprise networks and external networks must meet and maintain Department and Federal Information Technology compliance and data protection standards;*
- (4) DMZs should be segmented by Federal Information Processing Standard Publication 199 impact levels (moderate or low). Where feasible, applications and systems will be operated on the segment that matches their categorization impact level. Differences will be reconciled through the systems authorization process;*
- (5) Dual-home devices (e.g., servers with multiple network interface connections) must be approved on an individual basis through the Firewall Advisory Board (FAB); and*
- (6) Department approved multi-factor authentication is required for users with elevated privileges (e.g., system administrators).*

5 FAM 873.1 DMZ Registration

(CT:IM-155; 09-22-2014)

iMATRIX registration is required for each DMZ enclave (network segment) that will house a Department system. iMATRIX registration is required for systems and applications hosted within a DMZ enclave. An annual renewal of the registration by the system owner is required as part of the iMATRIX process (see 5 FAM 611). An annual Owner Accountability Form from the system owner to IRM/IA that certifies operation in accordance with established procedures is also required.

5 FAM 873.2 DMZ Assessment and Authorization

(CT:IM-155; 09-22-2014)

DMZs, systems residing within DMZs, and systems connecting to the DMZ must be authorized in accordance with the provisions of 5 FAM 1060, Information Assurance Management. IRM is authorized to disable systems that are deemed non-compliant or pose potential threats and have vulnerabilities that could impact the Departments information system's data and networks. Applicable Department security configuration standards must be applied and maintained by the system owners. For more information about security configuration standards, see the DS/SI/CS and IRM/IA OpenNet Web sites.

5 FAM 873.3 DMZ Hardware and Software

(CT:IM-155; 09-22-2014)

- a. All DMZ hardware and software must be approved by the enterprise Information Technology Configuration Control Board (IT CCB).*

UNCLASSIFIED (U)

U.S. Department of State Foreign Affairs Manual Volume 5
Information Management

- b. All IT hardware and software leveraged to support DMZs and the systems contained therein must comply with all federal laws and policies, including all federal accessibility laws and policies.*
- c. DMZ hardware and software must be configured to Department security configuration baseline standards, unless an exception is needed. System owners must submit requests for exceptions through DS/SI/CS and IRM/IA for a recommendation to receive approval for all deviations from approved configuration guides made to DMZ assets, and any deviations from approved configuration guides must be documented in iMATRIX. Only the CIO and/or Chief Information Security Officer (CISO) approve exceptions.*

5 FAM 874 THROUGH 879 UNASSIGNED